PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:)
)
Igor Garrievich Muttik) Art Unit: 2432
)
Application No. 10/755,450) Examiner: Lanier, Benjamin E.
)
Filed: 01/13/2004) Atty. Docket No.:
) NAI1P489/03.047.01
For: DETECTING MALICIOUS COMPUTER)
PROGRAM ACTIVITY USING EXTERNAL) Date: 03/05/2010
PROGRAM CALLS WITH DYNAMIC)
RULE SETS)
)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

REPLY BRIEF (37 C.F.R. § 41.37)

This Reply Brief is being filed within two (2) months of the mailing of the Examiner's Answer mailed on 01/05/2010.

Following is an issue-by-issue reply to the Examiner's Answer.

Issue # 1:

The Examiner has objected to the Specification as failing to provide proper antecedent basis for the claimed subject matter.

Specifically, the Examiner has argued that "[t]he phrase 'computer readable medium,' is not found to have proper antecedent basis in the specification" and that "[i]n order to overcome the objection, an amendment to the specification is necessary constituting a non-exhaustive statement of what the phrase 'computer readable medium' would be as it would have been known... in order to verify that the term... could not be taken in the context of non-statutory subject matter."

Appellant respectfully disagrees and notes that in Claim 1, appellant specifically claims "[a] computer program product embodied on a tangible computer readable medium" (emphasis added), which is clearly statutory. Additionally, appellant respectfully directs the Examiner's attention to Page 11, lines 14-16 and 21-23 of appellant's specification, which discloses that "computer program instructions... may be stored in one or more of the random access memory 204, the read only memory 206 and the hard disk drive 210" and that a "computer program may be stored and distributed on a recording medium or dynamically downloaded to the general purpose computer 200" (emphasis added), which are clearly examples of tangible computer readable mediums. Therefore, appellant's claimed "tangible computer readable medium" is clearly supported by the Specification, as claimed.

Of course, it should be noted that the above citations are merely examples of the above claim language and should not be construed as limiting in any manner.

In the Examiner's Answer mailed on 01/05/2010, on Page 4, the Examiner has not considered appellant's arguments "because the issue relates to petitionable subject matter under 37 CFR 1.181 and not to appealable subject matter," and has referred to MPEP §1002 and §1201.

Appellant respectfully disagrees and notes that MPEP §1002(a)(1) merely discloses that "[p]etition may be taken to the Director... [f]rom any action or requirement of any examiner in the *ex parte* prosecution of an application... which is not subject to appeal to the Board of Patent

Appeals and Interferences or to the court" (emphasis added), and MPEP §1002 generally discloses that "[p]etitions on appealable matters ordinarily are not entertained" (emphasis added). Additionally, appellant notes that MPEP §1201 discloses that "[w]here the differences of opinion concern the denial of patent claims because of prior art or **>other patentability issues<, the questions thereby raised are said to relate to the merits, and appeal procedure within the Office and to the courts has long been provided by statute" (emphasis added).

Therefore, the Examiner's objection to appellant's Specification with respect to appellant's claim language allegedly having improper antecedent basis constitutes a denial of one or more of appellant's patent claims because of a patentability issue, and as a result the appeal process is appropriate. In view of appellant's arguments hereinabove, appellant again respectfully notes that appellant's claimed "tangible computer readable medium" is clearly supported by the Specification, as claimed.

Issue # 2:

The Examiner has rejected Claims 1, 3-13, 15-18, 20-30, 32-35, 37-47, 49-52, and 55 under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement.

Group #1: Claims 1, 3-13, 15-18, 20-30, 32-35, 37-47, 49-52, and 55

Specifically, the Examiner has argued that "[t]he specification does not disclose how to detect whether the modified set of rules decreases malicious network traffic or slows malware propagation" and that "it is unclear how modified rules in one particular system has any effect on the amount of malicious traffic or the amount of propagated malware."

Appellant respectfully disagrees. First, appellant's claimed "determining whether said modified set of rules decreases malicious network traffic" and "determining whether said modified set of rules slows malware propagation" (see this or similar, but not necessarily identical language in the independent claims) is sufficiently enabled on Page 6, lines 4-12 of appellant's specification. For example, such excerpt discloses that "after a modified set is transmitted to other computers some network sensors detect the effect (e.g., decrease of traffic) and send a 'positive' signal back" (Page 6, lines 9-11), which clearly teaches how to detect whether the modified set of rules decreases malicious network traffic or slows malware propagation, as noted by the Examiner.

In the Examiner's Answer mailed on 01/05/2010, on Page 4, the Examiner has referred to MPEP 2164.01 and has cited numerous "factors to be considered when determining whether there is sufficient evidence to support a determination that a disclosure does not satisfy the enablement requirement and whether any necessary experimentation is 'undue'" from an unknown source. Additionally, on Page 5, the Examiner has argued the following:

> "Considering [a 'breadth of claims factor'], the claims require the use of one or more rules that are indicative of malicious computer program activity and subsequently modifying these rules. A determination is made as to whether these modified rules decreased malicious network traffic or whether these modified rules slowed malware propagation. The cited portion of the specification states that a 'report' signals whether or not the modified rules successfully decreased malicious network traffic or slowed malware propagation. The specification does not detail how this report is generated and what procedures were used to generate this report. Therefore, the skilled artisan would need to perform undue experimentation to perform the above mentioned determinations because the specification fails to provide even a hint of how the report is created or how the entire network's traffic is monitored."

Appellant respectfully disagrees. First, appellant respectfully notes that support for the disclosure in appellant's specification of "a report that modified rule(s) decrease the malicious network traffic or slowdown the malware propagation" (Page 6, lines 7-9) is clearly shown in the subsequent sentence of appellant's specification, where it is disclosed that "[a]s an example, after a modified set is transmitted to other computers some network sensors detect the effect (e.g., decrease of traffic) and send a 'positive' signal back" (Page 6, lines 9-11), where the "'positive' signal" is clearly an example of the aforementioned "report." This is reinforced by the disclosure in the specification that "an external signal could be a report" (Page 6, line 7 – emphasis added).

Therefore, since the specification clearly discloses an exemplary process of how the disclosed "report" may be generated (as a positive signal from a network sensor), a skilled artisan would not need to perform undue experimentation to determine how the report is created, as argued by the Examiner. Additionally, since the specification clearly illustrates an example where "network sensors detect the effect (e.g., decrease of traffic)" (Page 6, lines 9-11 – emphasis added), a skilled artisan would not need to perform undue experimentation to determine "how the entire network's traffic is monitored," as argued by the Examiner.

Additionally, in the Examiner's Answer mailed on 01/05/2010, on Pages 5-6, the Examiner has cited *In re Wands* and *In re Angstadt* and has further argued the following:

> "the specification is silent with respect to procedures performed to create the report. Therefore, in considering [a quantity of experimentation factor], the skilled artisan would need to perform a large quantity of experimentation to perform the claimed invention."

> "the specification provides no guidance with respect to the direction in which experimentation should proceed. Additionally, monitoring an entire network's traffic for a verifiable measure of malicious traffic and propagation cannot be considered routine."

Appellant respectfully disagrees. First, appellant again notes that appellant's specification does in fact clearly illustrate an exemplary procedure performed to create the report by disclosing that "network sensors detect the effect (e.g., decrease of traffic) and send a 'positive' signal back" (emphasis added), where the "positive" signal is clearly an example of a report, as shown hereinabove. Therefore, appellant asserts that the specification is not in fact "silent with respect to procedures performed to create the report," as argued by the Examiner, and that as a result, a large quantity of experimentation is unnecessary to perform the claimed invention.

Further, appellant notes that the Examiner has in fact cited from *Wands* the assertion that "a considerable amount of experimentation is permissible, if it is merely routine, or if the specification in question provides a reasonable amount of guidance with respect to the direction in which the experimentation should proceed" (emphasis added). However, since, as demonstrated by appellant hereinabove, a considerable amount of experimentation is not necessary in the present case, the question as to whether the considerable amount of experimentation is routine or whether the specification in question provides a reasonable amount of guidance with respect to the direction in which the experimentation should proceed is moot.

Further still, in the Examiner's Answer mailed on 01/05/2010, on Page 6, the Examiner has cited *In re Fisher* and has further argued the following with respect to "[t]he level of predictability in the art" and "[t]he amount of direction provided by the inventor":

> "Appellant's disclosure provides no guidance or direction on exactly how to make or use the invention. Therefore, the issue then becomes whether one skilled in the art can readily anticipate the effect of a change within the subject matter to which the claimed invention pertains. In the instant case, the unpredictable factors include the amount of malicious traffic and the amount of malware propagation. It is unclear how the skilled artisan would measure a change in the total amount of malicious traffic for an entire network based upon a modification of a set of rules. Likewise, it is unclear how the skilled artisan would measure a change in malware propagation based upon a modification to these same rules."

Appellant respectfully disagrees. Specifically, appellant again notes that, as shown hereinabove, appellant's specification (specifically, the disclosure in the specification of an exemplary process of how the disclosed "report" may be generated and sent as a positive signal from a network sensor) clearly provides guidance and direction as to "how to detect whether the modified set of rules decreases malicious network traffic or slows malware propagation," as noted by the Examiner. Therefore, the issue as to "whether one skilled in the art can readily anticipate the effect of a change within the subject matter to which the claimed invention pertains" is in fact moot.

Nevertheless, appellant notes that it is in fact clear that a skilled artisan may "measure a change in the total amount of malicious traffic [and malware propagation] for an entire network based upon a modification of a set of rules" since, as mentioned hereinabove, appellant's specification clearly teaches that "after a modified set is transmitted to other computers some network sensors detect the effect (e.g., decrease of traffic) and send a 'positive' signal back," where the "external signal could be a report that modified rule(s) decrease the malicious network traffic or slowdown the malware propagation" (Page 6, lines 7-11 – emphasis added). Therefore, appellant's disclosure of network sensors detecting an effect of a modified rule set and sending a signal back, where the signal can signify a decrease in the malicious network traffic or a slowdown the malware propagation, clearly illustrates "measur[ing] a change in the total amount of malicious traffic [and malware propagation] for an entire network based upon a modification of a set of rules," as noted by the Examiner.

Therefore, appellant again notes that the aforementioned excerpts from appellant's specification clearly teach how to detect whether the modified set of rules decreases malicious network traffic or slows malware propagation, as noted by the Examiner.

Additionally, in response to the Examiner's allegation that "it is unclear how modified rules in one particular system has any effect on the amount of malicious traffic or the amount of propagated malware," appellant respectfully points to Page 3, lines 17-25 of appellant's specification, which discloses that "[a secondary set of]external program calls logged in association with the primary set of external program calls known to correspond to malicious computer program activity may themselves subsequently be used as an indicator for malicious computer program activity," where "[t]he secondary sets of external program calls are 'tainted' by their association with the primary set of external program calls and the set of rules may be modified to be more sensitive to the secondary set of external program calls," and where "the set of rules associated with malicious computer program activity may be extended and the detection made potentially more sensitive, reliable and proactive" (emphasis added).

Therefore, in one embodiment, the modified set of rules may be more sensitive to additional external program calls, and may therefore be extended, resulting in more sensitive, reliable, and proactive detection, which may in turn decrease malicious network traffic and slow malware propagation.

In the Examiner's Answer mailed on 01/05/2010, on Page 7, the Examiner has argued the following:

> "Appellant's specification… discloses that the modification of the rules involves the modification of values assigned to each program call

> associated with the rules. When program code is monitored for malicious behavior, a log is maintained for all program calls made by the monitored code. Each program call has a specified value assigned and when the total value of all program calls made by the monitored code exceeds a predetermined threshold, the monitored code is considered malicious. The claimed modification of the rules simply modifies these values such that the total value of all program calls made by the monitored code is different from the previous set of rules. The modification of these rules has no effect on whether or not the monitored code is actually malicious. Therefore, the modification of these rules does not affect the actual amount of malicious traffic, or the actual amount of malware propagation, but instead merely modifies what the monitoring program considers to be malicious."

Appellant respectfully disagrees and again notes that appellant's specification teaches that "the set of rules associated with malicious computer program activity may be extended," resulting in "the **detection** [being] made potentially **more sensitive, reliable and proactive**" (Page 3, lines 23-25 – emphasis added). Additionally, appellant respectfully points to Page 2, lines 26-29 of appellant's specification, which discloses that "certain sequences of external program calls, or combinations of external program calls with certain characteristics, are indicative of malicious computer program activity and may be used to trigger anti-malware responses" (emphasis added). Further, appellant points to Page 2, lines 6-8 of appellant's specification, which discloses "detection of malicious computer program activity... using detected characteristics of external program calls" (emphasis added).

Therefore, appellant's specification discloses the detection of malicious activity as well as the triggering of anti-malware responses in response to external program calls, where such detection and triggering clearly affects "the actual amount of malicious traffic, or the actual amount of malware propagation," as noted by the Examiner, since the detecting of malicious activity and the triggering of and anti-malware response clearly result in a reduction of malicious traffic and malware propagation. Since such detection of malicious activity (and the resultant triggering of anti-malware responses) may be "made potentially more sensitive, reliable and proactive" as a result of a modified set of rules associated with malicious computer program activity, such modified set of rules clearly affects the amount of malicious traffic and malware propagation.

Again, with respect to the aforementioned excerpts from appellant's specification, it should be noted that the above citations are merely examples of the above claim language and should not be construed as limiting in any manner.

Issue # 3:

The Examiner has rejected Claims 1, 3-13, 15-18, 20-30, 32-35, 37-47, and 49-52 under 35 U.S.C. 112, second paragraph, as failing to particularly point out and distinctly claim the subject matter which appellant regards as the invention.

Group #1: Claims 1, 3-13, 15-18, 20-30, 32-35, 37-47, and 49-52

Specifically, the Examiner has argued that "[t]he term 'more strongly associated' is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention."

Appellant respectfully disagrees. First, appellant respectfully notes that appellant specifically claims "modifying said set of rules such that said at least one secondary set of one or more external program calls are more strongly associated with malicious computer program activity than said primary set of said one or more external program calls" (emphasis added - see this or similar, but not necessarily identical language in the independent claims). Therefore, appellant clearly claims that "said at least one secondary set… [is] more strongly associated with malicious computer program activity than said primary set" (emphasis added).

Additionally, appellant respectfully points to Page 4, lines 29-32 of appellant's specification, where it is disclosed that "a particularly convenient way of modifying the rule set [to] make it more sensitive to the secondary sets of external program calls is to increase the score values associated with such secondary sets of external program calls" (emphasis added). Additionally, Page 9, lines 21-26 of appellant's specification discloses "the generation of plurality of new rules which serve to more strongly associate the secondary sets of external program calls with malicious activity,” where “[t]he secondary sets themselves may not be sufficient to trigger the anti-malware response, but their score values are increased such that when they occur in combination with other detected behavioural characteristics an anti-malware response will now be triggered” (emphasis added). Therefore, in one embodiment, appellant’s claimed “at least one secondary set of one or more external program calls” is “more strongly associated with malicious computer program activity” by “increas[ing] the score values associated with such secondary sets of external program calls” (emphasis added).

As a result, appellant’s aforementioned claim language clearly is particularly pointed out and distinctly claimed. Again, it should be noted that the above citations are merely examples of the above claim language and should not be construed as limiting in any manner.

In the Examiner’s Answer mailed on 01/05/2010, on Page 8, the Examiner has argued the following:

> “Appellant’s disclosure does not provide a standard for measur[ing] the association of the claimed set of rules to malicious computer program activity. The claims require that the rules be modified such that a secondary set of program calls are ‘more strongly associated’ with malicious computer program activity than a primary set of program calls. Appellant’s specification (page 9, lines 20-29) explains that primary set of program calls is already associated with malicious activity when used to generate new/modified rules using secondary sets of program calls. Specifically, (page 9, lines 23-29)… appears to suggest that the rules are modified such that the secondary set of program calls is associated with malicious activity to the same extent that the primary set of program calls is associated with malicious activity. Therefore, the specification does not clearly define how the modified rules that include the secondary set of program calls is ‘more strongly associated’ to malicious activity than the primary set of program calls.”

Appellant respectfully disagrees. First, appellant points to Page 4, lines 22-26 of appellant’s specification, which discloses that “[a] particularly convenient way of structuring this rule set is to use score values associated with certain characteristics or combinations of characteristics of external program calls," where "[i]n this way, a logged stream may be analysed and when the total score value associated with that logged stream exceeds a threshold value, an anti-malware response may be triggered" (emphasis added). Additionally, as mentioned hereinabove, appellant's specification further discloses that one way of modifying a rule set to be more sensitive to secondary sets of program calls is to increase the score values associated with the secondary sets of program calls.

Therefore, since appellant's specification clearly discloses score values that are associated with characteristics of external program calls and which are used to trigger anti-malware responses once the score values exceed a threshold value, and discloses that increasing the score values associated with secondary sets of program calls of a rule set results in those secondary sets having higher score values that are closer to the triggering threshold value, and are therefore "more strongly associated with malicious computer program activity" (emphasis added). As such, appellant's specification does in fact "clearly define how the modified rules that include the secondary set of program calls is 'more strongly associated' to malicious activity than the primary set of program calls," as noted by the Examiner.

Further, as shown hereinabove, appellant's claimed "score values" clearly "provide a standard for measur[ing] the association of the claimed set of rules to malicious computer program activity," as noted by the Examiner. Additionally, "increas[ing] the score values associated with… secondary sets of external program calls" in order to "more strongly associat[e] [the secondary sets of external program calls] with malicious computer program activity" does not "suggest that the rules are modified such that the secondary set of program calls is associated with malicious activity to the same extent that the primary set of program calls is associated with malicious activity" (emphasis added) as alleged by the Examiner.

As such, appellant again notes that appellant's aforementioned claim language clearly is particularly pointed out in the specification and is distinctly claimed. Again, it should be noted that the above citations are merely examples of the above claim language and should not be construed as limiting in any manner.

Also, appellant's claimed "modifying said set of rules such that said at least one secondary set of one or more external program calls are more strongly associated with malicious computer program activity than said primary set of said one or more external program calls" (see this or similar, but not necessarily identical language in the independent claims) is purposefully drafted in a broad manner, and it would be unduly limiting for the Examiner to require appellant to specifically "provide a standard for ascertaining the requisite degree," as argued by the Examiner.

Additionally, the Examiner has argued that "it is unclear how modifying 'said set of rules' has any effect on a set of program calls that has already been logged, or the amount of malicious network traffic and malware propagation."

Appellant respectfully disagrees. First, appellant respectfully asserts that appellant's claims do not necessarily recite that a modified set of rules has an effect on a set of program calls that has already been logged, as suggested by the Examiner. For example, appellant claims "modifying code operable to modify said set of rules such that said at least one secondary set of one or more external program calls are more strongly associated with malicious computer program activity than said primary set of said one or more external program calls…wherein said set of rules is modified to include a new rule corresponding to said secondary set of one or more external program calls, said new rule thereafter being used in addition to other rules within said set of rules" (see this or similar, but not necessarily identical language in the independent claims).

Second, appellant points to Page 8, lines 8-11 and 17-21, which disclose one exemplary embodiment in which "checking is performed… which includes within its functionality the logging of a stream of external program calls, the identification of a primary set of program instruction calls found to match a rule or set of rules within the rules 10 and corresponding to malicious computer program activity," where "results associated with a particular external program call may also be examined and form part of the rule comparisons performed… in determining whether a particular external program call or set of external program calls matches one of the rules for identifying malicious computer program activity" (emphasis added).

Therefore, in one embodiment, results associated with an external program call may form part of rule comparisons that are performed for purposes of identifying malicious computer program activity. Thus, as shown hereinabove, appellant's aforementioned claim language clearly is particularly pointed out and distinctly claimed. Also, it should again be noted that the above citations are merely examples of the above claim language and should not be construed as limiting in any manner.

In the Examiner's Answer mailed on 01/05/2010, the Examiner has failed to respond to appellant's above arguments. Again, appellant notes that appellant's aforementioned claim language clearly is particularly pointed out in the specification and is distinctly claimed.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P489).

Respectfully submitted,

By: /KEVINZILKA/ Date: March 5, 2010
Kevin J. Zilka
Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660